COMP 754 — Cryptography & Security — Aj. Phillip Rogaway
Problem Set #3 — Out: 1 Aug 02 — Due: 13 Aug 02 (in class)

Problem 1 Let oracle $\mathcal{X}$ be an oracle that, on input x, returns a random integer in [1..10] other than x. Let $\mathcal{Y}$ be an oracle that, on input x, returns a random integer in [1..10]. Define the advantage of an adversary A is as $\mathbf{Adv}(A) = \Pr[A^{\mathcal{X}} = 1] - \Pr[A^{\mathcal{Y}} = 1]$. For each $q \geq 0$ define an adversary A_q that achieves maximal advantage. Compute the advantage of adversary A_{100}.

Problem 2 Fix an encryption scheme $\Pi = (\mathcal{E}, \mathcal{K}, \mathcal{D})$. Let $M_1, \ldots, M_{10}$ be fixed messages. Suppose you have an efficient adversary A that, given $C_1, \ldots, C_{10}, C$ determined by $C_i \xleftarrow{\$} \mathcal{E}_K(M_i)$, $M \xleftarrow{\$} \{0,1\}^8$, $C \xleftarrow{\$} \mathcal{E}_K(M)$, has an 10% chance to compute M. Describe an efficient adversary B that attacks Π and lower bound its advantage (in the ind-sense).

Problem 3 Consider the following block cipher $E : \{0,1\}^3 \times \{0,1\}^2 \to \{0,1\}^2$:

key	0	1	2	3
0	0	1	2	3
1	3	0	1	2
2	2	3	0	1
3	1	2	3	0
4	0	3	2	1
5	1	0	3	2
6	2	1	0	3
7	3	2	1	0

(The eight possible keys are the eight rows, and each row shows where points 0, 1, 2, and 3 map to.) Compute the maximal advantage an adversary can get, in the prp-sense, if A uses (a) one query, (b) two queries, and (c) four queries. Justify your answers.